抗不可信参与者的安全两方比较

赵搏文[1)] 祝遥[1)] 肖阳[2)] 裴庆祺[2)] 李小国[3)] 刘西蒙[4)]

[1)](西安电子科技大学广州研究院, 广州 510555, 广东省智能信息处理重点实验室, 深圳, 518060)
[2)](综合业务网理论及关键技术国家重点实验室,网络与信息安全学院,西安电子科技大学 西安 710126)
[3)](综合业务网理论及关键技术国家重点实验室,通信工程学院,西安电子科技大学, 西安 710126)
[4)](新加坡管理大学计算与信息系统学院, 新加坡 178902)
[5)](福州大学计算机与大数据学院, 福州 350108)

摘 要 安全两方比较被广泛用于构建各类安全计算协议，如安全机器学习训练和推理等. 现有的安全两方比较协议通常是一方先获知比较结果再将比较结果告知另一方，因此，难以防止先获知结果的参与方篡改比较结果. 为解决上述问题，本文首先提出一种抗不可信参与者的安全两方比较新范式. 随后，本文采用门限Paillier密码系统设计了一个满足新范式的安全两方比较协议. 该协议允许参与比较的两方在不泄露各自数据的情况下获得一致的比较结果，且协议保证任何一个参与者都不能篡改比较结果. 严格的理论分析证明表明本文所提协议是正确且安全的. 实验结果显示本文所提协议在计算效率上和功能上优于已有的安全两方比较方法. 相较于现有的安全两方比较方法，本文协议的计算效率提高了50倍.

关键词 安全比较；安全两方计算；同态加密；门限密码；可信计算

A Novel Two-Party Comparison Protocol Against Untrusted Parties

ZHAO Bo-Wen[1)] ZHU Yao[1)] XIAO Yang[2)] PEI Qing-Qi[3)] LI Xiao-Guo[4)] LIU Xi-Meng[5)]

[1)](Guangzhou Institute of Technology, Xidian University, Guangzhou 510555, Guangdong Key Laboratory of Intelligent Information Processing and Shenzhen Key Laboratory of Media Security, Shenzhen 518060)
[2)](State Key Lab of Integrated Service Networks, and the School of Cyber Engineering, and also with the Engineering Research Center of Trusted Digital Economy, Universities of Shaanxi Province, Xidian University, Xi'an, Shaanxi 710071.)
[3)](State Key Laboratory of Integrated Services Networks and Shaanxi Key Laboratory of Blockchain and Secure Computing, Xidian University, Xi'an 710071)
[4)](School of Computing and Information Systems, Singapore Management University, Singapore 178902)
[5)](College of Computer and Data Science, Fuzhou University, Fuzhou 350108)

Abstract

Secure two-party comparison is widely used to build various secure computing protocols (e.g., secure training, secure inference). In existing secure two-party comparison protocols, there is always one party that obtains a comparison result first, and then the party notifies the comparison result to the other one, thus, they are difficult to prevent one party that obtains the comparison result first from tampering with the comparison result. To this end, this paper first proposes a new paradigm for secure two-party comparison against untrusted parties. Then, a secure two-party comparison protocol (TOMS) satisfying the new paradigm is designed based on the threshold Paillier cryptosystem. Each party in TOMS obtains the same comparison result without revealing their own data. Moreover, TOMS prevents any party from tampering with the comparison results. Strictly theoretical analyses demonstrate the security and correctness of TOMS. Finally, the experimental results show that TOMS outperforms the existing secure two-party comparison methods in terms of computational efficiency and functionality, and is 50 times faster than previous methods.

Keywords secure comparison; secure two-party computation; homomorphic encryption; threshold cryptography; trusted computing

本课题得到国家重点研发计划项目(No. 2022YFB3102700)和国家自然科学基金(Nos. 62202358, 62102295, 62072109, U1804263, 61632013)资助. 赵搏文，男，博士，副教授，计算机学会（CCF）会员，主要研究领域为隐私计算及其应用. E-mail:bwinzhao@gmail.com. 祝遥（共同一作），男，硕士研究生，主要研究领域为隐私计算及其应用. 肖阳（通信作者），男，博士，讲师，计算机学会（CCF）会员，主要研究领域为智能安全、隐私保护. E-mail: yangtomas7@gmail.com. 裴庆祺，男，博士，教授，计算机学会（CCF）高级会员，主要研究领域为数字资产保护、网络安全. 李小国，男，博士，研究员，主要研究领域为：可信计算、隐私计算. 刘西蒙，男，博士，教授，计算机学会（CCF）高级会员，主要研究领域为安全计算、大数据安全等. 第1作者手机号码: 17688456313, E-mail: bwinzhao@gmail.com，zhaobowen@xidian.edu.cn

1 引 言

安全两方比较（secure two-party comparison）是指在没有可信第三方，且两个参与方在不透露各自输入数据x和y的情况下，输出x和y的大小关系[1]. 形式上，两个参与方Alice和Bob分别以x和y作为输入，以不泄露各自输入的方式共同执行比较函数$f(x,y)$并分别获得比较结果u_a和u_b，即，$(u_a,u_b)\leftarrow f(x,y)$.

安全两方比较问题最早源自姚期智院士1982年提出的百万富翁问题[1]，目前已成为安全多方计算领域中的关键技术. 百万富翁问题具体是指两个百万富翁在不透露双方具体财富数值的情况下比较谁更富有. 姚期智院士在提出百万富翁问题时提出了具体的解决方案，但其需要解密和验证操作的次数都是指数级的，导致其时间和空间复杂度花费巨大，现实应用的可能性较低. 为提高安全两方比较协议的实用性，姚期智院士于1986年提出基于混淆电路的安全两方计算方案[2].

此后，研究者们一直专注于设计更加高效的安全两方比较解决方案. Ioannidis等人[3]通过并行调用n轮2选1不经意传输协议来解决安全两方比较问题. 其中，n为输入数据的二进制表示位数，并且满足n^2小于不经意传输的安全参数大小，其运行效率较指数级的运算有所提升. Li等人[4]使用集合求交集判断元素大小的方法结合对称加密方法解决安全两方比较问题. 该方法使用对称加密提升协议效率，但在输入数据规模较大时其效率较低. Damgard[5]通过专用的DGK同态加密方案实现整数上的安全两方比较协议，该协议对比其他协议有着更为高效的运行效率，但是考虑到安全因素，其初始化时间较长，需要大约150秒. 目前，安全两方比较问题解决方案不仅考虑协议运行效率，也考虑协议的安全性. Li等人[6]使用ElGamal加密算法实现半诚实模型下的安全两方比较问题解决方案，并通过零知识证明和分割选择协议发现潜在的恶意行为，将该方案扩展到恶意模型下.

近年来，安全两方比较被广泛应用于拍卖隐私保护、机器学习、隐私保护外包计算和区间保密计算等领域[7–13]. Damle等人[7]提出一种安全两方比较问题的解决方案，并以此为基础提出组合拍卖协议TPACAS. 该协议相较于之前的工作可以保护代理隐私等与拍卖相关的隐私数据. Damle等人[8]进一步利用半受信任的第三方代理和以太坊提出一种可验证的安全两方比较问题解决方案，由此实现隐私保护的组合拍卖协议. Abspoel等人[9]提出一种基于勒让德符号的隐私比较协议并将其应用于安全神经网络分类器，结果显示在MNIST数据集上相较于MPyC内置安全比较协议效率提升约5倍. Liu等人[10]基于门限Paillier密码系统设计一种基于浮点数的隐私保护外包计算框架POCF. 基于安全两方比较思想，其子协议SLT（Secure Less Than Protocol）能判断两个密文数据之间的大小关系. Liu等人[11]使用零知识证明和Goldwasser–Micali加密算法及其异或同态等方法将区间保密计算问题（判断一个私密的有理数是否在一个私密的有理数区间内）转化为安全两方比较问题来解决. Guo等人[12]基于Paillier密码系统结合几何理论以及安全两方比较思想设计出一种高效的有理区间保密计算协议. 不仅如此，区间保密计算问题还可以扩展到点和线段、点和区域的包含问题. Zhao等人[13]设计一种密文上的安全两方比较协议，并在此基础上构造安全排序协议，解决集中式粒子群优化的关键步骤存在的隐私泄露问题，即从所有粒子选择典范时泄露任何粒子的私有数据的问题.

尽管研究者们在提升安全两方比较协议性能和应用安全两方比较协议上做出诸多努力，但都忽视了不可信的参与方可以篡改比较结果，从而破坏协议的可靠性. 不失一般性，现有的安全两方比较协议总是让参与比较两方中的一方（如，Alice）先获得比较结果u_a，再由Alice通知Bob比较结果u_b. 如果Alice是可信的，Alice设置$u_b=u_a$. 此时，Alice和Bob获得相同的比较结果. 如果Alice是不可信的，Alice设置$u_b\neq u_a$. 此时，Bob将不能获得正确的比较结果. 因此，目前的安全两方比较协议难以解决下述问题：

问题: Alice和Bob两个富翁都看中一处房产并约定资产多的人才有最终购买权，且双方都不愿意向其他人透露其总资产. 直观上，采用现有的安全两方比较协议可以解决该问题. 但是由于先获知比较结果的富翁（如，Alice）极易欺骗另一个富翁（如，Bob）. 在这种情况下，两个富翁Alice和Bob难以确信谁才有最终购买权.

为解决上述问题，本文研究抗不可信参与者的安全两方比较方法. 技术上，该方法将保证参与比较的两方Alice和Bob以私有数据x和y作为输入，执行安全两方比较协议$(u_a,u_b)\leftarrow f(x,y)$后，Alice和Bob总是获得相同的比较结果（即，$u_a=u_b$总成立），且Alice和Bob都不能篡改比较结果. 本文的技术贡献可归纳为三个方面：

(1) 提出一种新型抗不可信参与者的安全两方比较范式，该范式规定参与比较的两方获知相同的比较结果，且任何一方都不能篡改比较结果.

(2) 设计一种抗不可信参与者的安全两方比较协议，该协议利用门限Paillier密码系统密钥的可

拆分性和安全两方计算的思想，实现防止不可信参与者的安全两方比较.

(3) 协议安全且高效. 严格的理论分析证明任何参与者篡改比较结果是计算不可行的. 同等实验条件下，本文提出协议的计算速度是同类方法的50倍.

本文的剩余部分组织如下：第2章介绍安全两方比较问题的研究现状；第3章提出抗不可信参与者的安全两方比较范式；第4章首先给出门限Paillier密码系统，接着，详细描述抗不可信参与者的安全两方比较协议的系统模型和威胁模型及其具体设计；第5章证明所提出的安全协议满足选择明文攻击（Chosen-plaintext attack，CPA）安全，并证明协议满足抗不可信参与者的安全两方比较范式；第6章通过实验对比现有的安全两方比较协议，评估协议的效率及可行性；第7章总结全文.

2 相关工作

基于安全两方比较协议构造所采用的底层技术，本节简要回顾基于混淆电路的安全两方比较方法、基于同态加密的安全两方比较方法、以及基于秘密共享的安全两方比较方法.

基于混淆电路的安全两方比较方法. 该方法将安全两方比较问题转化为混淆电路（garbled circuit）的形式解决. ObliVM[14]通过编译一种ObliVM-lang的类java语言，由此实现内置的高效ORAM方案，提升半诚实模型下安全两方计算的效率. ABY[15]是一种半诚实模型下基于C++库的混合协议框架，通过不同协议之间相互转化的机制，开发者可以实现对计算效率的细粒度控制. ObliVM和ABY都提供基于混淆电路（经free-xor优化[16]）的通用安全两方计算问题解决方案，都能解决安全两方比较问题. 当协议中存在恶意参与者时，通过分割选择方法（cut-and-choose）能有效防止其恶意行为. 在分割选择方法中，发送方构造并发送多个混淆电路给接收方，接收方随机验证部分混淆电路的正确性，若检查到存在错误则说明发送方存在恶意行为. Canetti[17]等人通过分割选择的方法确保结果的正确性. 但该方法要求构造大量电路，其计算和空间复杂度较高，实用性较差.

基于同态加密的安全两方比较方法. 由于同态加密对密文的运算能够映射到明文上，使其能够在保护隐私数据的同时完成安全两方计算任务，所以该方法十分契合安全两方比较的需求. Lin等人[18]结合ElGamal同态加密方案和字符串集合求交集的大小比较方法，通过比较两方的0编码和1编码并用ElGamal同态加密方案保证1编码的保密性，由此解决安全两方比较问题. Liu等人[19]提出两方和多方安全比较问题的解决方案，通过将财富值转化为向量表示并结合Paillier密码系统的同态性解决安全两方比较问题. Li等人[20]提出半诚实模型和恶意模型下的最大（小）值比较协议，通过ElGamal同态加密方案、向量化表示财富值和零知识证明等方法解决两方或多方比较问题. Liu等人[21]基于门限Paillier密码方案提出一套在自然数上的隐私保护外包计算方法POCR. 其子协议SLT能判断两个密文的大小关系，解决了安全两方比较问题. Zhao等人[22]改进Liu的相关工作，提出整数上的安全外包计算方法SOCI，其子协议SCMP不仅支持整数上的密文比较，且能够抵抗选择明文攻击. 本文提出的抗不可信参与者的安全两方比较协议是在SCMP上改进得到的.

基于秘密分享的安全两方比较方法. Nishide[23]提出一种有效的比特位分解协议，通过比特位的秘密分享实现安全两方比较. 文献[19]将财富值向量化，使用秘密分享的方法替代Paillier同态加密保护数据隐私，降低计算复杂度，实现安全多方比较. Damgard[24]提出一种将某一特定秘密的多项式共享转化为比特共享的方法，通过调用秘密共享方案的乘法协议实现高效安全两方比较.

表1从功能上比较本文所提协议和现有典型方案，由论文[20]提出的semiSMC采用同态加密技术，论文[19]提出的semiSSC采用秘密分享技术，实现安全两方比较. ObliVM [14]采用混淆电路构造安全两方比较协议. ABY [15]对比ObliVM [15]优化在线阶段协议耗时，实现更高效的两方比较协议. 技术上，ObliVM和ABY都不能防止不可信的参与者篡改比较结果. 本文提出的抗不可信参与者的安全两方比较协议（TOMS *）可以防止不可信的参与者.

表1 安全两方计算方案的比较

方法	底层技术	抗不可信参与者	效率
ObliVM [14]	混淆电路	否	中
ABY [15]	混淆电路	否	高
semiSSC [19]	秘密分享	否	高
semiSMC [20]	同态加密	否	低
TOMS	同态加密	是	高

3 抗不可信参与者的安全两方比较范式

如图1所示，在理想的安全两方比较中，参与者Alice和Bob分别拥有私有数据x和y. 互相不信任

*TOMS: **T**w**O**-party co**M**parison protocol against Untru**S**ted parties

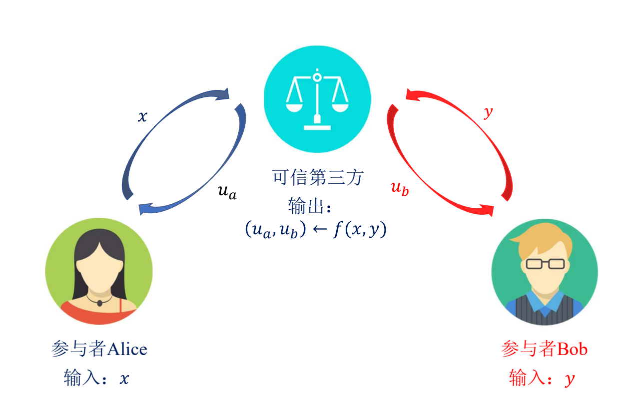


图1 理想的安全两方比较.

的Alice和Bob通过可信第三方联合执行安全两方比较函数$(u_a, u_b) \leftarrow f(x, y)$得出$x$和$y$之间的大小关系，在协议执行过程中双方不泄露自己的输入数据并且都能获得正确的结果u_a和u_b，且$u_a = u_b$.

定义1. 假定两个参与方Alice和Bob分别以私有数据x和y作为输入，共同执行两方安全比较协议$f(x, y)$并分别获得比较结果u_a和u_b. 抗不可信参与者的安全两方比较协议范式满足如下特性：

- **机密性**. 安全两方比较协议$f(x, y)$执行完成后，参与协议的Alice能确保自己的输入数据x不会泄露给Bob. 反之亦然.
- **正确性**. 安全两方比较协议执行$f(x, y)$完成后，参与协议的Alice和Bob分别获得比较结果u_a和u_b，且$u_a = u_b$总成立. 换而言之，Alice和Bob总是获得相同的比较结果.
- **可靠性**. 安全两方比较协议执时，先得到结果的参与方（如Alice）不能篡改比较结果u_b，使$u_b \neq u_a$，且后获得结果的参与方（如Bob）容易发现Alice是否篡改过比较结果.

4 抗不可信参与者的安全两方比较协议

本节简要介绍门限Paillier密码系统. 接着，描述TOMS的系统模型，威胁模型以及详细设计. 最后分析TOMS的正确性.

4.1 门限Paillier密码系统

本文描述一种$(2, 2)$门限Paillier密码系统，其包含：密钥生成、加密、解密、密钥拆分、部分解密和门限解密算法. $(2, 2)$门限Paillier密码系统与传统Paillier密码系统[25]的主要区别在于前者将Paillier密码系统的私钥拆分成两个部分私钥.

密钥生成(Key Generation，KeyGen)：令k为安全参数，且p，q为大素数，满足$|p| = |q| = k$，其中，$|x|$代表x的二进制位数. 随后计算$N = p \cdot q$，$\lambda = (p-1)(q-1)/2$和$\mu = \lambda^{-1} \bmod N$. 定义函数$L(x) = \frac{x-1}{N}$，并选取生成元$g = N + 1$. 最后得到公钥$pk = (N, g)$，以及与之对应的私钥$sk = \lambda$.

加密(Encryption，Enc)：输入明文消息$m \in \mathbb{Z}_N$，输出其对应密文$[\![m]\!]$. 具体加密算法如下：

$$[\![m]\!] = \mathbf{Enc}(pk, m) = g^m r^N \bmod N^2.$$

其中，r从$\mathbb{Z}_N^*$中随机选取.

解密(Decryption，Dec)：输入密文消息$[\![m]\!]$，通过私钥$sk = \lambda$解密后输出对应明文m，具体解密算法如下：

$$m = \mathbf{Dec}(sk, [\![m]\!]) = L([\![m]\!]^\lambda \bmod N^2)\mu \bmod N.$$

密钥拆分(Private Key Splitting，KeyS)：输入私钥$sk = \lambda$，输出拆分后的私钥sk_1和sk_2. 具体地，将私钥拆分为两个部分，分别为$sk_1 = \lambda_1$和$sk_2 = \lambda_2$，满足$\lambda_1 + \lambda_2 \equiv 0 \bmod \lambda$，且$\lambda_1 + \lambda_2 \equiv 1 \bmod N$. 根据中国剩余定理[26]，可以计算得出满足$\delta \equiv 0 \bmod \lambda$，且$\delta \equiv 1 \bmod N$的$\delta = \lambda_1 + \lambda_2 = \lambda \cdot \mu \bmod (\lambda \cdot N)$. 此时，选择$\lambda_1$为$\sigma$比特的随机数，$\lambda_2 = \lambda \cdot \mu + \eta \cdot \lambda N - \lambda_1$，其中$\eta$为非负整数.

部分解密(Partial Decryption，PDec)：输入密文消息$[\![m]\!]$和部分私钥sk_i（$i \in \{1, 2\}$），输出部分解密的结果M_i，具体部分解密算法如下：

$$M_i = \mathbf{PDec}([\![m]\!], sk_i) = [\![m]\!]^{\lambda_i} \bmod N^2.$$

门限解密(Threshold Decryption，TDec)：输入一对部分解密的结果M_1，M_2，输出其对应的明文m. 具体门限解密算法如下：

$$m = \mathbf{TDec}(M_1, M_2) = L(M_1 \cdot M_2 \bmod N^2).$$

门限Paillier密码系统的加法同态性和标量乘法同态性表现如下：

- 加法同态性：$\mathbf{Dec}(sk, [\![m_1 + m_2 \bmod N]\!]) = \mathbf{Dec}(sk, [\![m_1]\!] \cdot [\![m_2]\!])$.
- 标量乘法同态性：$\mathbf{Dec}(sk, [\![c \cdot m \bmod N]\!]) = \mathbf{Dec}(sk, [\![m]\!]^c)$，其中，$c \in \mathbb{Z}_N$.

4.2 系统模型

如图2所示，TOMS包括两个参与者Alice和Bob，他们分别有私有数据x和y. 不失一般性，为保护参与方的私有数据，Alice采用(2,2)门限Paillier密码系统设置密钥参数，Bob采用传统Paillier密码系统生成密钥参数. 具体地，

- 参与者Alice：Alice首先调用密钥生成算法**KeyGen**产生一个公私钥对(pk_a, sk_a)，其中$pk_a = (N_a, g_a)$. 此外，Alice调用**KeyS**拆分

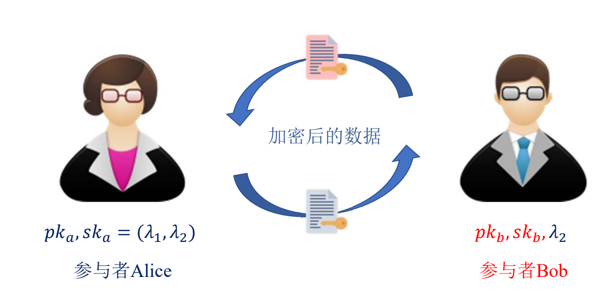


图2　系统模型.

私钥sk_a生成两个部分私钥λ_1和λ_2，并将拆分后的部分私钥λ_2和Alice的公钥分发给Bob.

- 参与者Bob：Bob调用密钥生成算法**KeyGen**产生一个Paillier密码系统的公私钥对(pk_b, sk_b)，其中$pk_b = (N_b, g_b)$，并将Bob的公钥分发给Alice.

4.3　威胁模型

在抗不可信参与者的安全两方比较协议中总共包含两个实体，分别是参与者Alice和参与者Bob. 本文假定Alice和Bob均为半诚实的，即Alice和Bob严格遵循并执行协议，但会通过协议执行过程中的中间值等信息来获取另一参与方的输入数据. 半诚实敌手Alice和Bob的目标是获取对方的输入数据或篡改对方获得的最终比较结果. 具体的恶意行为如下：

(1)半诚实敌手Alice通过协议执行过程中Bob发送的消息来推断出Bob的输入数据y.

(2)半诚实敌手Bob通过协议执行过程中Alice发送的消息来推断出Alice的输入数据x.

(3)半诚实敌手Alice作为先得到比较结果的一方可能会篡改正确的比较结果u_b（使$u_b \neq u_a$），并将篡改后的u_b告知Bob.

4.4　详细设计

本文假定$x, y \in [-2^\ell, 2^\ell]$，其中，$\ell$是一个整数且满足$2^\ell \ll N$，如$\ell = 32$.

TOMS的详细过程如图3. Alice输入数据x 并维护(pk_a, sk_a)以及$(\lambda_1, \lambda_2) \leftarrow$ **KeyS**(sk_a). Bob输入数据y并维护(pk_b, sk_b). 其中，$x, y \in [-2^\ell, 2^\ell]$.

TOMS的工作流程如图3所示，TOMS以Alice和Bob的私有数据x和y作为输入，输出x和y的比较结果u_a和u_b. 形式上，TOMS可以表示为$(u_a, u_b) \leftarrow \mathcal{F}(x, y)$，其中，$\mathcal{F}$是一个安全两方比较函数且满足抗不可信参与者的安全两方比较范式. 如图3所示，TOMS的5个步骤详细流程如下：

（1）Bob按加密私有数据y成$[\![y]\!]_{pk_b} = \mathbf{Enc}(pk_b, y)$，并将加密结果$[\![y]\!]_{pk_b}$发送给Alice.

（2）Alice加密私有输入x成$[\![x]\!]_{pk_b} = \mathbf{Enc}(pk_b, x)$. 随后，Alice随机选择$s \in \{0, 1\}$，并通过如下计算得到$D$：

$$D = \begin{cases} \left([\![x]\!]_{pk_b} \cdot [\![y]\!]_{pk_b}^{N_b - 1}\right)^{r_1} \cdot [\![r_1 + r_2]\!]_{pk_b}, & 若 s = 0 \\ \left([\![y]\!]_{pk_b} \cdot [\![x]\!]_{pk_b}^{N_b - 1}\right)^{r_1} \cdot [\![r_2]\!]_{pk_b}, & 若 s = 1 \end{cases} \tag{1}$$

其中，r_1从集合$\{0,1\}^\sigma \backslash \{0\}$中随机选取，$r_2$从集合$\{0,1\}^\kappa \backslash \{0\}$中随机选取（$\sigma, \kappa$为安全参数，且$\ell < \sigma < \kappa < |\frac{N_b}{2}|$），随机选取的$r_1$和$r_2$满足以下条件：

$$\begin{cases} r_2 \le \frac{N_b}{2}, \\ r_1 + r_2 > \frac{N_b}{2}. \end{cases} \tag{2}$$

然后，Alice加密s成$[\![s]\!]_{pk_a} = \mathbf{Enc}(pk_a, s)$，并调用部分解密算法部分解密$[\![s]\!]_{pk_a}$得到$M_1 = \mathbf{PDec}([\![s]\!]_{pk_a}, \lambda_1)$. 最后，Alice将$D$，$[\![s]\!]_{pk_a}$和$M_1$发送给Bob.

（3）Bob收到D，$[\![s]\!]_{pk_a}$和M_1后，首先解密D获得$d = \mathbf{Dec}(sk_b, D)$. 若$d > \frac{N_b}{2}$，记$u_1 = 0$，否则记$u_1 = 1$. 随后，Bob加密$u_1$成$[\![u_1]\!]_{pk_a} = \mathbf{Enc}(pk_a, u_1)$. 最后，Bob将$[\![u_1]\!]_{pk_a}$发送给Alice.

（4）Alice收到$[\![u_1]\!]_{pk_a}$后，首先解密$[\![u_1]\!]$获得u_1，并计算$u_a = s - u_1$. 随后，Alice将λ_2发送给Bob.

（5）Bob获得λ_2后，部分解密$[\![s]\!]_{pk_a}$获得$M_2 = \mathbf{PDec}([\![s]\!]_{pk_a}, \lambda_2)$. 随后，Bob计算$s = \mathbf{TDec}(M_1, M_2)$. 最后，Bob计算$u_b = s - u_1$.

4.5　正确性分析

参与者Alice能获得正确的比较结果. 在第（2）步中，输入数据$x, y \in [-2^\ell, 2^\ell]$，随机数$r_1$从$\{0,1\}^\sigma \backslash \{0\}$中随机选择，随机数$r_2$从$\{0,1\}^\kappa \backslash \{0\}$中随机选择，满足$r_2 \le \frac{N_b}{2}$，且$r_1 + r_2 > \frac{N_b}{2}$. 根据$s$的不同取值，分类讨论如下：

- 若$s = 0$. 易知$x - y + 1 \in [-2^{\ell+1} + 1, 2^{\ell+1} + 1]$，$D$的解密结果$d = r_1(x - y + 1) + r_2 \in [\frac{N_b}{2} + 2 - 2^{\sigma+\ell+1} - 2^\sigma, \frac{N_b}{2} + 2^{\sigma+\ell+1} + 2^\sigma]$. Alice在第（4）步中得到$u_1$（若$d \ge \frac{N_b}{2}$，$u_1 = 0$. 若$d < \frac{N_b}{2}, u_1 = 1$）. 由$\frac{N_b}{2} \gg 2^{\sigma+\ell+1}(\ell < \sigma < \kappa < |\frac{N_b}{2}|)$，$0 < d < N_b$以及$r_1$和$r_2$的选取条件可得：

  （1）当$x \ge y$时，易知$d = r_1(x - y + 1) + r_2 \ge \frac{N_b}{2}$，所以$u_1 = 0$. 此时$u_a = s - u_1 = 0 - 0 = 0$. 由TOMS的输出可得$u_a = 0$代表$x \ge y$. 因此，Alice能获得正确的比较结果.

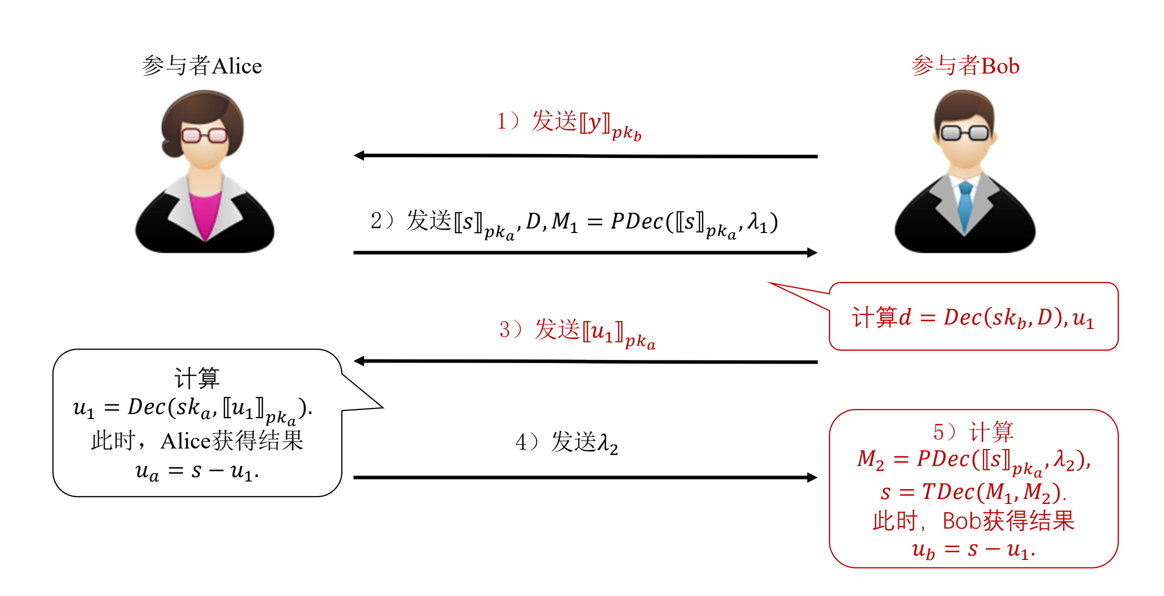


图3 TOMS流程图.

（2）当$x < y$时，易知$d = r_1(x-y+1)+r_2 < \frac{N_b}{2}$，所以$u_1 = 0$. 此时$u_a = s - u_1 = 0 - 1 = -1 = N_b - 1\,(mod\,N_b)$. 由于$u_a > \frac{N_b}{2}$，所以$u_a = N_b - u_a = 1$. 由TOMS的输出可得$u_a = 1$代表$x < y$. 因此，Alice能获得正确的比较结果.

- 若$s = 1$. 易知$y - x \in [-2^{\ell+1}, 2^{\ell+1}]$，$d = r_1(y-x) + r_2 \in [\frac{N}{2} + 2 - 2^{\sigma+\ell+1} - 2^{\sigma}, \frac{N}{2} + 2^{\sigma+\ell+1} + 2^{\sigma}]$. 同理可得：

  （1）当$x \geq y$时，易知$d < \frac{N_b}{2}$，所以$u_1 = 1$. 此时$u_a = s - u_1 = 1 - 1 = 0$. 由TOMS的输出可得$u_a = 0$代表$x < y$. 因此，Alice能获得正确的比较结果.

  （2）当$x < y$时，易知$d \geq \frac{N_b}{2}$，所以$u_1 = 0$. 此时$u_a = s - u_1 = 1 - 0 = 1$. 由TOMS的输出可得$u_a = 1$代表$x < y$. 因此，Alice能获得正确的比较结果.

综上所述，Alice总能获得正确的比较结果.

参与者Bob能获得正确的安全比较结果. Bob在第（1）步中发送y的加密结果给Alice. Bob在第（3）步中通过解密输入D获得d，再通过d与$\frac{N_b}{2}$的关系求出u_1，并得到经加密的$[\![s]\!]_{pk_a}$以及$[\![s]\!]_{pk_a}$的部分解密结果M_1. Bob在第（5）步时收到Alice的拆分私钥λ_2后部分解密$[\![s]\!]_{pk_a}$的到M_2. 然后联合M_1在门限解密算法**TDec**(M_1, M_2)的作用下得到s. 由于TOMS执行到第（4）步时Alice能获得正确的安全两方比较结果u_a，且Bob和Alice生成u_b和u_a所需s和u_1是相同的，所以Bob能获得正确的安全两方比较结果$u_b = s - u_1$.

由于$u_a = s - u_1$且$u_b = s - u_1$，因此，$u_a = u_b$总成立. 换句话说，Alice和Bob总是获得相同的比较结果.

5 安全性分析

本节首先介绍选择明文攻击（chosen-plaintext attack, CPA）安全性定义，并证明TOMS第（2）步中使用的加密方案$r_1(x-y+1)+r_2$或$r_1(y-x)+r_2$满足CPA安全性（为了简洁，令$m = x-y+1, y-x$）. 随后给出半诚实模型下的安全性定义，并通过半诚实模型下的模拟范式证明了TOMS的安全性. 最后，验证TOMS满足抗不可信参与者的安全两方比较范式.

5.1 CPA安全定义

CPA安全通常使用计算上不可区分性实验来描述[27]，在实验中共有两个角色：敌手$\mathcal{A}$攻击系统，挑战者$\mathcal{C}$对敌手的行为进行反馈. 实验$\text{PubK}^{CPA}_{\mathcal{A},r_1m+r_2}(\sigma,\kappa)$具体过程如下：

(1) 敌手$\mathcal{A}$随机选择两个消息m_0和m_1发送给挑战者$\mathcal{C}$.

(2) 挑战者$\mathcal{C}$随机选择比特$b \in \{0,1\}$，并生成随机数r_1和r_2，计算$r_1m_b + r_2$发送给敌手$\mathcal{A}$.

(3) 敌手$\mathcal{A}$输出一个比特$b' \in \{0,1\}$当做对b的猜测.

(4) 若$b = b'$，则实验结果为1，即$\text{PubK}^{CPA}_{\mathcal{A},r_1m+r_2}(\sigma,\kappa) = 1$，代表着敌

手$\mathcal{A}$攻击成功. 若$b \neq b'$，则实验结果为0，即$\mathrm{PubK}^{CPA}_{\mathcal{A},r_1m+r_2}(\sigma,\kappa)=0$，代表着敌手$\mathcal{A}$攻击失败.

定义2. 若加密方案r_1m+r_2满足：对于任意概率多项式时间敌手$\mathcal{A}$都存在一个关于σ和κ的可忽略函数$negl(\sigma,\kappa)$，使得以下不等式成立：

$$\Pr\left[\mathrm{Pubk}^{cpa}_{\mathcal{A},r_1m+r_2}(\sigma,\kappa)=1\right] \leq \frac{1}{2}+negl(\sigma,\kappa)$$

则说明加密方案r_1m+r_2是CPA安全的.

定理1. 对于$m_0,m_1 \in [-2^\ell,2^\ell]$，$r_{10},r_{11} \in [2^{\sigma-1},2^\sigma-1]$以及$r_{20},r_{21} \in [2^{\kappa-1},2^\kappa-1]$满足$r_{10}m_0+r_{20}$和$r_{11}m_1+r_{21}$在计算上是不可区分的（例如，$\ell=64,\sigma=128,\kappa=512$）. 形式上，挑战者$\mathcal{C}$随机选取$m_b \in [-2^\ell,2^\ell]$（$b\in\{0,1\}$），$r_1 \in [2^{\sigma-1},2^\sigma-1]$和$r_2 \in [2^{\kappa-1},2^\kappa-1]$计算$r_1m_b+r_2$. 此时对于敌手$\mathcal{A}$，通过$r_1m_b+r_2$推测出$b'$，使得$b'=b$（$b'\in\{0,1\}$）的概率$\Pr\left[b'=b \mid r_1m_b+r_2\right] \leq \frac{1}{2}+negl(\kappa)$，其中$negl(\kappa)$为关于$\kappa$的可忽略函数. 说明加密方案$r_1m+r_2$满足CPA安全.

证明. 随机选择$m_b \in [-2^\ell,2^\ell]$，$r_1 \in [2^{\sigma-1},2^\sigma-1]$和$r_2 \in [2^{\kappa-1},2^\kappa-1]$，所以$r_1m_b+r_2 \in \left[2^{\kappa-1}-2^{\ell+\sigma}+2^\ell,2^\kappa+2^{\ell+\sigma}-2^\ell-1\right]$. 由于$r_1$和$r_2$是挑战者$\mathcal{C}$在实验$\mathrm{PubK}^{CPA}_{\mathcal{A},r_1m+r_2}(\sigma,\kappa)$第(2)步中随机选择的，所以$r_1m_b+r_2$随机分布在$\left[2^{\kappa-1}-2^{\ell+\sigma}+2^\ell,2^\kappa+2^{\ell+\sigma}-2^\ell-1\right]$范围内. 即敌手$\mathcal{A}$从$r_1m_b+r_2$中推断出$b$的概率为$\Pr\left[b'=b \mid r_1m_b+r_2\right]=\frac{1}{2}$.

当敌手$\mathcal{A}$在实验$\mathrm{PubK}^{CPA}_{\mathcal{A},r_1m+r_2}(\sigma,\kappa)$第（1）步中选择$m_0=-2^\ell$，$m_1=2^\ell$时，敌手$\mathcal{A}$推断出$b$的概率最高，具体如下：

- 若挑战者$\mathcal{C}$在实验$\mathrm{PubK}^{CPA}_{\mathcal{A},r_1m+r_2}(\sigma,\kappa)$第（2）步选择$b=0$，则当$r_1m_b+r_2 \in \left[2^{\kappa-1}-2^{\ell+\sigma}+2^\ell,2^{\kappa-1}+2^{\ell+\sigma-1}-1\right]$时，敌手$\mathcal{A}$能推断出$b'=b=0$的概率为1.
- 若挑战者$\mathcal{C}$在实验$\mathrm{PubK}^{CPA}_{\mathcal{A},r_1m+r_2}(\sigma,\kappa)$第（2）步选择$b=1$，则当$r_1m_b+r_2 \in \left[2^\kappa-2^{\ell+\sigma-1},2^\kappa+2^{\ell+\sigma}-2^\ell-1\right]$时，敌手$\mathcal{A}$能推断出$b'=b=1$的概率为1.

综合考虑以上两种情况，敌手$\mathcal{A}$攻击成功的概率最大为：

$$\begin{aligned}&\Pr\left[b'=b \mid r_1m_b+r_2\right]\\ =&\frac{1}{2}+\frac{1}{2}\cdot\frac{2^{\kappa-1}+3\cdot 2^{\ell+\sigma-1}-2^\ell-1+1-2^{\kappa-1}}{2^{\kappa-1}}\\ &+\frac{1}{2}\cdot\frac{2^\kappa+3\cdot 2^{\ell+\sigma-1}-2^\ell-1+1-2^\kappa}{2^{\kappa-1}}\\ =&\frac{1}{2}+\frac{3\cdot 2^{\ell+\sigma}-2^{\ell+1}}{2^\kappa}\end{aligned}$$

由ℓ,σ,κ之间的大小关系（$\ell<\sigma<\kappa$）可知，$2^\kappa \gg 3\cdot 2^{\ell+\sigma}-2^{\ell+1}$，所以存在可忽略函数$negl(\kappa)=\frac{3\cdot 2^{\ell+\sigma}-2^{\ell+1}}{2^\kappa}$使得：

$$\Pr\left[b'=b \mid r_1m_b+r_2\right] \leq \frac{1}{2}+negl(\sigma,\kappa)$$

证毕.

5.2 半诚实模型下的安全性定义

在半诚实模型下，协议中的参与者都是半诚实的. 半诚实的参与者会按协议的相关要求诚实地执行协议，但是在协议执行的过程中会记录对方发送过来的消息序列和自己抛硬币（coin tosses）产生的结果. 协议执行完后半诚实的参与者会根据自己记录的所有中间结果来推断出其他参与者的隐私信息.

安全两方计算理想模型. 记$f:\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*\times\{0,1\}^*$是一个概率多项式时间函数，代表着安全两方计算的随机计算过程. 其中，$f(x,y)=(f_1(x,y),f_2(x,y))$. 在两方参与的理想模型下，Alice和Bob双方分别拥有输入数据x和y，通过可信的第三方（Trusted Third Party, TTP）计算函数$f(x,y)$. 协议执行完成后，Alice和Bob分别得到$f_1(x,y)$和$f_2(x,y)$),并且不泄露各自的输入数据x和y. 具体定义如下：

（1）Alice将自己的输入数据x发送给TTP.

（2）Bob将自己的输入数据y发送给TTP.

（3）TTP通过x和y计算$f(x,y)=(f_1(x,y),f_2(x,y))$. 计算完成后将$f_1(x,y)$发送给Alice，将$f_2(x,y)$发送给Bob.

特别的，由于TTP是诚实的，参与者除了从TTP获得自己相应的$f_i(x,y)(i\in\{1,2\})$之外，得不到任何其他信息，所以理想协议是最安全的协议，在理想模型下能解决任何安全两方计算问题. 若一个实际协议能够达到与理想协议相同的安全性，则可以说明该实际协议是安全的.

模拟范式 模拟范式是一种广泛接受的证明多方（两方）安全计算协议安全性的方法. 模拟范式通过对比理想模型与现实情况下的多方（两方）安全计算协议来定义协议的安全性，若现实情况下协议泄露的信息不会多于理想模型下泄露的信息，则

可以说明该协议是安全的.

具体地，若协议执行过程中的某一参与者获得的消息等同于从其输入和输出推断出来的消息，则说明该协议是安全的. 安全两方计算协议使用模拟范式来形式化表达协议安全性，通过协议的输入和输出来模拟参与方的视图，并且参与方从输出中无法获得其他信息.

假设参与方Alice拥有输入数据x，参与方Bob拥有输入数据y，双方通过安全两方计算协议π联合计算一个概率多项式时间函数$f(x,y) = (f_1(x,y), f_2(x,y))$. 在执行协议$\pi$的过程中，定义Alice和Bob双方获得的视图分别为$\text{view}_1^\pi(x,y) = (x, r, m_1, \ldots, m_t)$和$\text{view}_2^\pi(x,y) = (y, r', m'_1, \ldots, m'_t)$. 其中，Alice和Bob执行协议时收到的消息序列分别为$(m_1, \ldots, m_t)$和$(m'_1, \ldots, m'_t)$. Alice和Bob执行协议时抛硬币得到的结果分别为r和r'. 最终，Alice和Bob完成协议后得到的结果分别为 $\text{output}_1^\pi(x,y)$和 $\text{output}_2^\pi(x,y)$[28].

定义3. 对于特定函数f，如果存在概率多项式时间算法S_1和S_2（一般称S_1和S_2为模拟器.）满足以下条件：

$$\begin{aligned}&\{(S_1(x, f_1(x,y)), f_2(x,y))\}_{x,y}\\&\overset{c}{\equiv}\left\{\left(\text{view}_1^\Pi(x,y),\ \text{output}_2^\Pi(x,y)\right)\right\}_{x,y}\\&\{(S_2(y, f_2(x,y)), f_1(x,y))\}_{x,y}\\&\overset{c}{\equiv}\left\{\left(\text{view}_2^\Pi(x,y),\ \text{output}_1^\Pi(x,y)\right)\right\}_{x,y}\end{aligned}\tag{3}$$

则说明协议π保密计算了函数f. 其中，$\overset{c}{\equiv}$代表着计算上的不可区分性.

5.3 安全性证明

定理2. 抗不可信参与者的安全两方比较协议在半诚实条件下是安全的.

证明. 依照定义3要求，分别构造模拟器S_1和S_2，若两个模拟器使公式(3)成立，即可证明定理2的正确性. 在TOMS中，$f_1(x,y) = u_a, f_2(x,y) = u_b$

下面分别讨论构造模拟器S_1和S_2的两种情况.

构造模拟器S_1. 具体的模拟流程如下：

（1）S_1随机选取$y' \in [-2^\ell, 2^\ell]$，使得$f_1(x,y) = f_1(x,y') = u_a$. 随后加密$y'$得到$[\![y']\!]_{pk_b} = \textbf{Enc}(pk_b, y')$.

（2）S_1随机选取$r_1 \in \{0,1\}^\sigma \backslash \{0\}$，$r_2 \in \{0,1\}^\kappa \backslash \{0\}$和$s \in \{0,1\}$. 随后加密$s$得到$[\![s]\!]_{pk_a} = \textbf{Enc}(pk_a, s)$，部分解密$[\![s]\!]_{pk_a}$得到$M_1 = \textbf{PDec}([\![s]\!]_{pk_a}, \lambda_1)$. 若$s = 0$，计算$D' = \left([\![x]\!]_{pk_b} \cdot [\![y']\!]_{pk_b}^{N_b - 1}\right)^{r_1} \cdot [\![r_1 + r_2]\!]_{pk_b}$. 若$s = 1$，则计算$D' = \left([\![y']\!]_{pk_b} \cdot [\![x]\!]_{pk_b}^{N_b - 1}\right)^{r_1} \cdot [\![r_2]\!]_{pk_b}$.

（3）S_1解密D'得到$d' = \textbf{Dec}(sk_b, D')$. 若$d' > \frac{N_b}{2}$，记$u'_1 = 0$，否则记$u'_1 = 1$. 随后加密$u'_1$得到$[\![u'_1]\!]_{pk_a} = \textbf{Enc}(pk_a, u'_1)$.

（4）S_1解密$[\![u'_1]\!]_{pk_a}$得到$u'_1 = \textbf{Dec}(sk_a, [\![u'_1]\!]_{pk_a})$，随后计算$u'_a = s - u'_1$.

（5）S_1部分解密$[\![s]\!]_{pk_a}$得到$M_2 = \textbf{PDec}([\![s]\!]_{pk_a}, \lambda_2)$. 随后完全解密$[\![s]\!]_{pk_a}$得到$s = \textbf{TDec}(M_1, M_2)$，最后计算$u'_b = s - u'_1$.

结合上述模拟步骤，模拟器S_1得到的视图为$S_1(x, f_1(x,y)) = (x, [\![x]\!]_{pk_b}, s, [\![y']\!]_{pk_b}, [\![s]\!]_{pk_a}, M_1, M_2, D', d', u'_1, f_1(x,y'))$. 真实视图$\text{view}_1^\Pi(x,y) = (x, [\![x]\!]_{pk_b}, s, [\![y]\!]_{pk_b}, [\![s]\!]_{pk_a}, M_1, M_2, D, d, u_1, f_1(x,y))$. 模拟器$S_1$得到的结果 $\text{output}_2^\Pi(x,y) = u'_b$，真实的结果$f_2(x,y) = u_b$. 由于$f_1(x,y) = f_1(x,y')$，所以$u_a = u'_a$，从而$u_1 = u'_1$，进一步得出$d = d'$以及 $\text{output}_2^\Pi(x,y) \overset{c}{\equiv} f_2(x,y)$. 又因为Paillier加密是语义安全的，所以$[\![y]\!]_{pk_b} \overset{c}{\equiv} [\![y']\!]_{pk_b}$，且$D \overset{c}{\equiv} D'$.

即存在模拟器S_1满足：

$$\begin{aligned}&\{(S_1(x, f_1(x,y)), f_2(x,y))\}_{x,y}\\&\overset{c}{\equiv}\left\{\left(\text{view}_1^\Pi(x,y),\ \text{output}_2^\Pi(x,y)\right)\right\}_{x,y}\end{aligned}\tag{4}$$

构造模拟器S_2. 具体的模拟流程如下：

（1）S_2随机选取$\bar{x} \in [-2^\ell, 2^\ell]$，使得$f_2(x,y) = f_2(\bar{x},y) = u_a$. 随后加密$y$得到$[\![y]\!]_{pk_b} = \textbf{Enc}(pk_b, y)$.

（2）S_2随机选取$\bar{r_1} \in \{0,1\}^\sigma \backslash \{0\}$，$\bar{r_2} \in \{0,1\}^\kappa \backslash \{0\}$和$\bar{s} \in \{0,1\}$. 随后加密$\bar{s}$得到$[\![\bar{s}]\!]_{pk_a} = \textbf{Enc}(pk_a, \bar{s})$，部分解密$[\![\bar{s}]\!]_{pk_a}$得到$\bar{M_1} = \textbf{PDec}([\![\bar{s}]\!]_{pk_a}, \lambda_1)$. 若$\bar{s} = 0$，计算$\bar{D} = \left([\![\bar{x}]\!]_{pk_b} \cdot [\![y]\!]_{pk_b}^{N_b - 1}\right)^{\bar{r_1}} \cdot [\![\bar{r_1} + \bar{r_2}]\!]_{pk_b}$. 若$\bar{s} = 1$，则计算$\bar{D} = \left([\![y]\!]_{pk_b} \cdot [\![\bar{x}]\!]_{pk_b}^{N_b - 1}\right)^{\bar{r_1}} \cdot [\![\bar{r_2}]\!]_{pk_b}$.

（3）S_2解密$\bar{D}$得到$\bar{d} = \textbf{Dec}(sk_b, \bar{D})$. 若$\bar{d} > \frac{N_b}{2}$，记$\bar{u_1} = 0$，否则记$\bar{u_1} = 1$. 随后加密$\bar{u_1}$得到$[\![\bar{u_1}]\!]_{pk_a} = \textbf{Enc}(pk_a, \bar{u_1})$.

（4）S_2解密$[\![\bar{u_1}]\!]_{pk_a}$得到$\bar{u_1} = \textbf{Dec}(sk_a, [\![\bar{u_1}]\!]_{pk_a})$，随后计算$\bar{u_a} = \bar{s} - \bar{u_1}$.

（5）S_2部分解密$[\![\bar{s}]\!]_{pk_a}$得到$\bar{M_2} = \textbf{PDec}([\![\bar{s}]\!]_{pk_a}, \lambda_2)$. 随后完全解密$[\![\bar{s}]\!]_{pk_a}$得到$\bar{s} = \textbf{TDec}(\bar{M_1}, \bar{M_2})$,最后计算$\bar{u_b} = \bar{s} - \bar{u_1}$.

结合上述模拟步骤，模拟器S_2得到的视图为$S_2(y, f_2(x,y)) = (y, [\![y]\!]_{pk_b}, [\![\bar{x}]\!]_{pk_b}, \bar{s}, [\![\bar{s}]\!]_{pk_a}, \bar{M_1}, \bar{M_2}, \bar{D}, \bar{d}, \bar{u_1}, f_1(\bar{x},y))$，真实视图$\text{view}_1^\Pi(x,y) = (y, [\![y]\!]_{pk_b}, [\![x]\!]_{pk_b}, s, [\![s]\!]_{pk_a}, M_1, M_2, D, d, u_1, f_1(x,y))$. 模拟器$S_2$得到的结果 $\text{output}_1^\Pi(x,y) = \bar{u_a}$，真实的结果$f_1(x,y) = u_a$.

由于$f_2(x,y)=f_2(\bar{x},y)$，所以$u_b=\bar{u_b}$，进一步可以推导出$\bar{s}\overset{c}{\equiv}s$，$\bar{u_1}\overset{c}{\equiv}u_1$以及 $\text{output}_1^{\Pi}(x,y)\overset{c}{\equiv}f_1(x,y)$. 由于Paillier加密是语义安全的，所以$[\![\bar{x}]\!]_{pk_b}\overset{c}{\equiv}[\![x]\!]_{pk_b}$，$[\![\bar{s}]\!]_{pk_b}\overset{c}{\equiv}[\![s]\!]_{pk_b}$和$[\![\bar{u_1}]\!]_{pk_b}\overset{c}{\equiv}[\![u_1]\!]_{pk_b}$，进一步推导出$M_1\overset{c}{\equiv}\bar{M_1}$和$M_2\overset{c}{\equiv}\bar{M_2}$. 最后，由定理1可知：$d=\bar{d},D\overset{c}{\equiv}\bar{D}$.

即存在模拟器S_2满足：

$$\begin{aligned}&\{(S_2\left(y,f_2(x,y)\right),f_1(x,y))\}_{x,y}\\ \overset{c}{\equiv}&\left\{\left(\text{view}_2^{\Pi}(x,y),\ \text{output}_1^{\Pi}(x,y)\right)\right\}_{x,y}.\end{aligned}\quad(5)$$

证毕.

以上方案证明TOMS在半诚实模型下是安全的，并且能抵抗选择明文攻击. 接下来进一步验证TOMS满足抗不可信参与者的安全两方比较范式，即，验证TOMS满机密性，正确性和可靠性.

机密性. Alice和Bob双方的输入数据都不会泄露.

- 对于Alice，其输入数据x不会泄露给Bob，理由如下：在TOMS第（2）步中，Alice通过Paillier密码系统B计算d（若$s=0$，$d=r_1(x-y+1)+r_2$，若$s=1$，$d=r_1(y-x)+r_2$）的加密值D. 随后，在TOMS第（3）步中，Bob通过自己持有的私钥sk_b解密D得到d. 根据定理1，加密方案r_1m+r_2是CPA安全的，所以Bob不能通过d获取Alice的输入数据x.
- 对于Bob，其输入数据y不会泄露给Alice，理由如下：在TOMS第（1）步中，Bob加密y得到$[\![y]\!]_{pk_b}$. 由于Alice没有私钥sk_b，所以Alice无法获通过$[\![y]\!]_{pk_b}$取Bob的输入数据y.

正确性. 4.5节已详细证明协议的正确性，避免重复，此处不再复述.

可靠性. 在TOMS中，Alice作为先得到最终比较结果u_a的一方，可靠性保证敌手Alice不能篡改Bob获得的最终比较结果u_b，保证$u_a=u_b$始终成立. 由于Bob获得的最终比较结果$u_b=s-u_1$，结合TOMS的第（2）和（3）步，敌手Alice通过改变d的值影响u_1（若$d\geq\frac{N_b}{2}$，则$u_1=0$，否则$u_1=1$），并最终影响Bob的解密结果u_b.

在上述分析中，Alice通过选取特定的d'来改变半诚实参与方的最终结果u_b. 所以，要证明TOMS满足抗不可信参与者的安全两方比较的可靠性，只需证明d和d'是计算上不可区分的. 根据定理1，加密方案$d=r_1m+r_2$（若$s=0$，$d=r_1(x-y+1)+r_2$. 若$s=1$，$d=r_1(y-x)+r_2$）满足CPA安全，即，d和d'是计算上不可区分的. 所以，对于$d=r_1(y-x)+r_2$（$d=r_1(x-y+1)+r_2$），敌手Alice不能通过选取特定的d'来改变半诚实参与方的最终结果u_b. 即，敌手Alice不能改变半诚实参与方的最终结果u_b，所以TOMS满足抗不可信参与者的安全两方比较范式的可靠性.

综上，TOMS满足抗不可信参与者的安全两方比较范式.

6 实验评估

本节实验对比ObliVM[14]，ABY[15]，TOMS和semiSMC[20]在实现安全两方比较协议的性能，并测试不同安全参数N和明文长度ℓ下TOMS的运行效率.

实验配置. 测试时具体实验环境配置为：Intel（R）Core（TM）i5-8300H CPU 2.30GHz；内存16GB；操作系统Windows11 64位；编程环境：C++和GMP6.2.

6.1 效率分析

一般通过计算复杂度和通信复杂度来衡量具体协议的效率. 且在考虑计算复杂度时，由于模指数运算的计算复杂度远大于其他运算. 例如计算g^r需要$1.5|r|$次模乘运算[27]（其中，$|r|$表示其二进制表示位数），所以通常忽略其他运算，只考虑协议执行过程中的模指数运算次数. 考虑到参与双方在协议执行前可以进行产生和交换密钥操作，所以对协议进行效率分析时不考虑准备阶段. 表2给出不同协议之间的计算复杂度、通信复杂度的比较.

计算复杂度. 根据TOMS的执行过程，具体的计算复杂度分析如下（具体实验时$N_a=N_b=N$）：（1）Bob加密生成$[\![y]\!]_{pk_b}$需要$1.5|N|$次模乘运算.（2）Alice加密x和s共需要$3|N|$次模乘运算，生成D需要$1.5|N|+3\sigma$次模乘运算，部分解密$[\![s]\!]_{pk_a}$需要1.5σ次模乘运算；（3）Bob解密求出u_1需要$1.5|N|$次模乘运算，加密u_1得到$[\![u_1]\!]_{pk_a}$需要$1.5|N|$次模乘运算；（4）Alice解密u_1共需$1.5|N|$次模乘运算；（5）Bob部分解密$[\![s]\!]_{pk_a}$共需要1.5σ次模乘运算；综上，TOMS计算复杂度为$10.5|N|+6\sigma$.

semiSMC解决多方求最大值的问题. 本文设置参与方为两方，由此对比两方安全比较. 具体地，在加密阶段两个参与者共需要$6v|N|$次模乘法运算，在解密阶段找到最小值平均需要$1.5v|N|$次模指数运算，且找到最大值平均需要$1.5v|N|$次模指数运算. 所以，总共需要$9v|N|$次模指数运算，其中参与方的输入从一个集合中选取，v代表该集合的大小，N为使用公钥加密方案的模数. 如表2所示，因为v代表参与方输入集合的大小. 由

于安全性的原因，$v \gg 2$，又因为$|N| \gg \sigma$，所以TOMS的计算复杂度低于同类方法semiSMC. ABY混合算术共享、布尔共享和混淆电路解决安全多方计算问题，但在本实验中仅使用混淆电路. 具体地，ABY和ObliVM在本文设置中仅使用经free-xor优化后混淆电路实现两方安全比较，计算复杂度依赖于电路中与门（AND）的数量，且计算时仅使用廉价的共享密钥计算（异或门（XOR）计算仅需本地进行异或操作，忽略计算开销）.

特别的，基于混淆电路的ObliVM和ABY两种方案计算复杂度与其对应电路的与门数量相关，难以与本文提出的基于同态加密的TOMS进行对比，所以其计算复杂度用⊥替代. 后续实验结果证明本文提出的TOMS在计算效率上是最优的.

通信复杂度. 通信复杂度具体取决于通信轮数和通信开销. 在通信轮数方面，ObliVM和ABY两种基于混淆电路（ABY是混合协议，但在本实验中仅使用混淆电路）的协议通信轮数为4. 具体地，Alice传输混淆表和自己输入数据对应标签需要1轮通信，随后Bob通过并行执行不经意传输协议来获取输入数据每一比特对应的标签需要2轮通信，最后传输结果需要1轮通信. semiSMC协议运行时需要向其他参与方公布自己数据的编码向量，所以其通信轮数为$n(n-1)$，n为参与方数量. 易知，TOMS使用4轮通信.

在通信开销方面，semiSMC所有参与方都要传输定义域集合内所有元素的加密值，所以TOMS的通信开销远低于同类方法semiSMC. 并且对比基于混淆电路的OBliVM和ABY协议，TOMS的通信开销也是最低的. 具体地，TOMS，semiSMC，ObliVM和ABY的通信开销分别为1.25KB，49.9KB，14.8KB和10.29KB.

表2　不同协议的计算与通信复杂度比较

方法	计算复杂度	通信轮数	通信开销
ObliVM[14]	⊥	4	14.80 KB
ABY[15]	⊥	4	10.29 KB
semiSMC[20]	$9v\|N\|$	$n(n-1)$	49.90 KB
TOMS	$10.5\|N\|+6\sigma$	4	1.25 KB

⊥：实验中ABY仅使用混淆电路，与ObliVM在计算复杂度上都与其生成电路的与门数量相关.

6.2　实验测试

在实验中，我们使用预计算提升TOMS协议的运行效率. 例如，Alice在协议执行前预先计算TOMS第（2）步中的$[\![s]\!]_{pk_a}$，$[\![r_1+r_2]\!]_{pk_a}$，$[\![r_2]\!]_{pk_a}$等变量，等到TOMS执行时直接使用预计算的结果，无需在协议执行过程中计算.

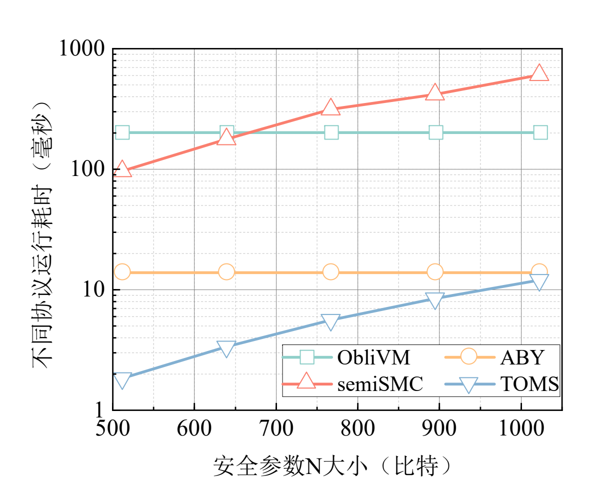


图4　32比特明文在不同安全参数下协议运行时间.

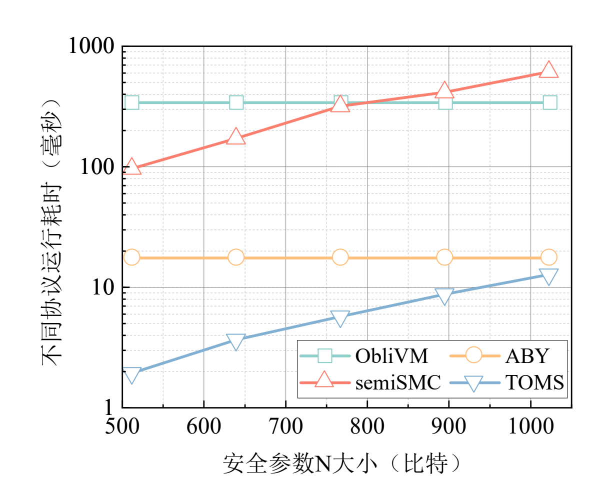


图5　64比特明文在不同安全参数下协议运行时间.

实验1测试不同明文长度ℓ与不同安全参数N大小下ObliVM，ABY，semiSMC，TOMS协议的运行效率. 其中，安全参数N具体是指TOMS与semiSMC采用加密方案的模数. 具体地，在TOMS中$\sigma=128$，$N_a=N_b=N$，且使用预计算优化. 在semiSMC中输入方集合大小$v=200$，在ABY中仅使用姚氏混淆电路，所以设置$sharing=S_YAO$.

明文长度$\ell=32$比特，安全参数N的范围从512比特到1024比特时，不同协议具体其执行时间（单位毫秒）具体如图4. 明文长度为$\ell=64$比特，安全参数N的范围从512比特到1024比特时，不同协议具体其执行时间如图5.

如图4所示，由于ObliVM和ABY采用混淆电路实现安全两方比较，其运行时间与安全参数N无关，所以二者在明文长度$\ell=32$比特下，协议运行时间不变分别为200.8毫秒和13.9毫秒. 其次是随着安全参数N的增加，TOMS和semiSMC计算

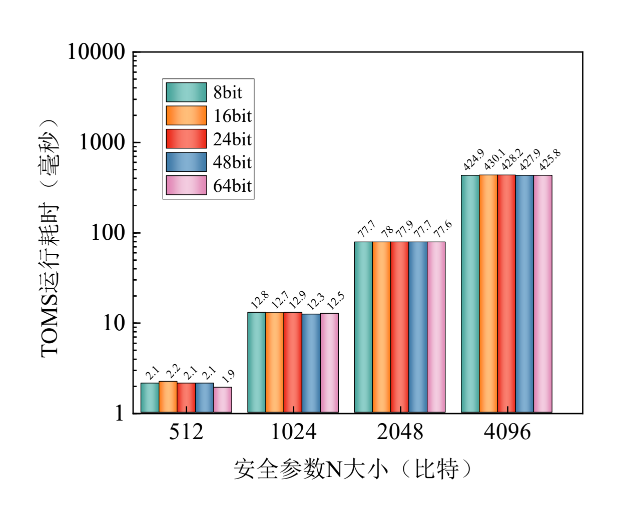


图6　不同安全参数和明文大小下TOMS的运行时间.

单次模幂运算耗时增加，TOMS和semiSMC的运行时间逐步增加，且semiSMC较TOMS的上升趋势更显著（semiSMC的计算复杂度大于TOMS）. 最后在协议运行时间上，本文提出的TOMS表现最优，在$N = 1024$比特时，相较于ObliVM快189毫秒，相较于ABY快2.1毫秒. 特别的，相较于同类方法semiSMC快592毫秒（51.2倍）.

如图5所示，由于电路大小和通信总量与明文长度ℓ正相关，所以明文长度ℓ越大，其耗时越多. 具体地，明文长度$\ell = 64$比特，ObliVM和ABY的运行时间分别是340.1毫秒和17.5毫秒，相较于32比特明文，运行时间分别增加139.6毫秒和3.6毫秒. 其次是对比图4，TOMS在相同安全参数下，明文长度$\ell = 32$比特和明文长度$\ell = 64$比特的运行时间一致（差距在2毫秒左右），semiSMC同样如此. 其原因是Paillier加密算法加密明文时存在随机的乘法因子r，导致其明文长度与其对应的密文大小无关，进一步导致明文长度与协议运行时间无关. 最后在协议运行时间上，本文提出的TOMS表现最优，在$N = 1024$比特时，相较于ObliVM快327.6毫秒，相较于ABY快5毫秒. 特别的，相较于同类方法semiSMC快598毫秒（48.8倍）.

实验2测试不同安全参数和明文比特对TOMS效率的影响. 具体地，明文长度ℓ比特范围从8到64比特，安全参数$\sigma = 128$，$N_a = N_b = N$分别为512，1024，2048，4096比特. 具体协议执行时间如图6.

如图6所示，在某一具体安全参数N取值下，TOMS执行时间不受明文大小影响. 例如，当$N = 1024$时，明文长度ℓ比特范围从8到64比特，协议执行时间都为12.8毫秒左右. 当$N = 2048$时，明文从8到64比特，协议执行时间都为78毫秒左右. 其次是随着安全参数N的增大，TOMS运行时间也成倍增加. 从$N = 512$到$N = 1024$，TOMS运行时间增加约6.4倍. 从$N = 1024$到$N = 2048$，TOMS运行时间增加约6.1倍. 从$N = 2048$到$N = 4096$，TOMS运行时间增加约5.5倍.

实验1和2结果表明TOMS在半诚实模型且安全参数$N = 1024$时，运行效率高于基于混淆电路的ObliVM和ABY，以及基于同态加密的semiSMC. 综上，TOMS在满足抗不可信参与者的安全两方比较范式的同时，保证协议运行效率.

7　结 论

为解决现有的安全两方比较协议无法抵抗不可信参与者的问题，本文提出一种抗不可信参与者的两方比较协议. 具体地，本文首先形式地定义抗不可信参与者的安全两方比较范式，并通过门限Paillier密码系统设计一个满足抗不可信参与者的安全两方比较范式的安全两方比较协议TOMS. 相比于现有的安全两方比较协议，TOMS不仅极大地提高安全两方比较协议效率的同时，并且协议保证任何一方都无法篡改比较结果并使得每个参与方都获得一致的比较结果. 未来，我们将尝试将抗不可信参与者的安全两方比较范式扩展到抗不可信参与者的的安全多方通用计算.

参 考 文 献

[1] YAO A C. Protocols for secure computations//23rd annual symposium on foundations of computer science (sfcs 1982), 1982: 160-164.

[2] YAO A C. How to generate and exchange secrets//27th Annual Symposium on Foundations of Computer Science (sfcs 1986), 1986: 162-167.

[3] Ioannidis I, GRAMA A. An efficient protocol for yao's millionaires' problem//36th Annual Hawaii International Conference on System Sciences, 2003: 6-pp.

[4] Li S D, DAOSHUN W, YIQI D, et al. Symmetric cryptographic solution to yao's millionaires' problem and an evaluation of secure multiparty computations. Information Sciences, 2008, 178(1): 244-255.

[5] DAMGARD I, GEISLER M, KROIGARD M. Homomorphic encryption and secure comparison. International Journal of Applied Cryptography, 2008, 1 (1): 22-31.

[6] Li S D, Wang W L, Du R M. Protocol for millionaires' problem in malicious model. Scientia Sinica Informationis, 2021, 51(01): 75-88.

(李顺东, 王文丽, 杜润萌. 抗恶意敌手的百万富翁问题解决方案[J]. 中国科学: 信息科学, 2021, 51(01): 75-88.)

[7] DAMLE S, FALTINGS B, GUJAR S. A practical solution to yao's millionaires' problem and its application in designing secure combinatorial auction. arXiv preprint arXiv:1906.06567, 2019.

[8] DAMLE S, FALTINGS B, GUJAR S. Blockchain-based practical multi-agent secure comparison and its application in auctions//International Conference on Web Intelligence and Intelligent Agent Technology, 2021: 430-437.

[9] ABSPOEL M, BOUMAN N J, SCHOENMAKERS B, et al. Fast secure comparison for medium-sized integers and its application in binarized neural networks// Cryptographers' Track at the RSA Conference, 2019: 453-472.

[10] LIU X, DENG R H, DING W, et al. Privacy-preserving outsourced calculation on floating point numbers. IEEE Transactions on Information Forensics and Security, 2016, 11(11): 2513-2527.

[11] LIU X, ZHANG R, XU G, et al. Confidentially judging the relationship between an integer and an interval against malicious adversaries and its applications. Computer Communications, 2021, 180: 115-125.

[12] Guo Y M, Zhou S F, Dou J W, et al. Efficient privacy-preserving interval computation and its applications. Chinese Journal of Computers, 2016 (39): 1-17.

(郭奕, 周素芳, 窦家维, 等. 高效的区间保密计算及应用. 计算机学报, 2016 (39): 1-17.)

[13] Zhao B, Liu X, Song A, et al. PRIMPSO: A Privacy-Preserving Multiagent Particle Swarm Optimization Algorithm. IEEE Transactions on Cybernetics, 2022.

[14] LIU C, WANG X S, NAYAK K, et al. Oblivm: A programming framework for secure computation//2015 IEEE Symposium on Security and Privacy, 2015: 359-376.

[15] DEMMLER D, SCHNEIDER T, ZOHNER M. Aby-a framework for efficient mixed-protocol secure two-party computation.//NDSS, 2015.

[16] KOLESNIKOV V, SCHNEIDER T. Improved garbled circuit: Free xor gates and applications//International Colloquium on Automata, Languages, and Programming, 2008: 486-498.

[17] RAN C, POBURINNAYA O, VENKITASUBRAMANIAM M. Equivocating yao: constant-round adaptively secure multiparty computation in the plain model//the 49th Annual ACM SIGACT Symposium, 2017.

[18] LIN H Y, TZENG W G. An efficient solution to the millionaires' problem based on homomorphic encryption// International Conference on Applied Cryptography and Network Security, 2005: 456-466.

[19] LIU X, LI S, CHEN X, et al. Efficient solutions to two-party and multiparty millionaires' problem. Security and Communication Networks, 2017, 2017.

[20] Li S D, Xu W T, Wang W L, et al. Secure Maximum (Minimum) Computation in Malicious Model. Chinese Journal of Computers, 2021, 44(10): 2076-2089.

(李顺东, 徐雯婷, 王文丽, 等. 恶意模型下的最大(小)值保密计算. 计算机学报, 2021, 44(10): 2076-2089.)

[21] LIU X, CHOO K K R, DENG R H, et al. Efficient and privacy-preserving outsourced calculation of rational numbers. IEEE Transactions on Dependable and Secure Computing, 2016, 15(1): 27-39.

[22] ZHAO B, YUAN J, LIU X, et al. SOCI: A toolkit for secure outsourced computation on integers. IEEE Transactions on Information Forensics and Security, 2022, 17: 3637-3648.

[23] NISHIDE T, OHTA K. Multiparty computation for interval, equality, and comparison without bit-decomposition protocol//International Workshop on Public Key Cryptography, 2007: 343-360.

[24] DAMGÅRD I, FITZI M, KILTZ E, et al. Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation//Theory of Cryptography Conference, 2006: 285-304.

[25] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes//International conference on the theory and applications of cryptographic techniques, 1999: 223-238.

[26] PEI D, SALOMAA A, DING C. Chinese remainder theorem: applications in computing, coding, cryptography. World Scientific, 1996.

[27] KATZ J, LINDELL Y. Introduction to modern cryptography. CRC press, 2020.

[28] ODED G. Foundations of cryptography: volume 2, basic applications. Cambridge university press, 2009.



ZHAO Bo-Wen received his Ph.D. degree in cyberspace security from South China University of Technology, China, in 2020. Now, he is a associate professor at Guangzhou Institute of Technology, Xidian University, Guangzhou. His current research interests include privacy-preserving computation.

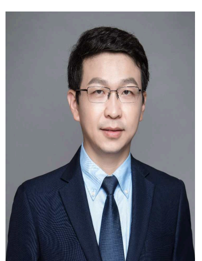


ZHU Yao received the B.S. degree from the school of Computer Science, Hubei University of Technology. He is currently pursing the M.S. degree with Guangzhou Institute of Technology, Xidian University. His research interests include privacy-preserving computation and its application.



XIAO Yang received the B.S. and Ph.D. degrees in communication engineering from Xidian University, Xi'an, China, in 2013 and 2020, respectively. From 2017 to 2019, he was supported by the China Scholarship Council to be a Visiting Ph.D. Student with the University of New South Wales, Sydney, New South Wales, Australia. He is currently a Lecturer with the State Key Laboratory of Integrated Services Networks, School of Cyber

Engineering, Xidian University. His research interests include social networks, joint recommendations, graph neural network, trust evaluation, and blockchain.



PEI Qing-Qi received his Ph.D. degrees in Computer Science and Cryptography from Xidian University, in 2008. He is now a Professor and member of the State Key Laboratory of Integrated Services Networks, also Senior Member of Chinese Institute of Electronics and China Computer Federation. His research interests focus on digital contents protection and wireless networks and security.



LI Xiao-Guo received the PhD degree in computer science from Chongqing University, China, in 2019. He worked at Hong Kong Baptist University as a Postdoctoral Research Fellow from 2019-2021. He is currently a Research Fellow at Singapore Management University, Singapore. His current research interests include trusted computing, secure computation, and public-key cryptography.



LIU Xi-Meng received the Ph.D. degree in Cryptography from Xidian University, China, in 2015. Now he is the full professor in the College of Computer Science and Data Science, Fuzhou University. Also, he was a research fellow at Peng Cheng Laboratory, Shenzhen, China. He awards "Minjiang Scholars" Distinguished Professor, "Qishan Scholars" in Fuzhou University, and ACM SIGSAC China Rising Star Award (2018). His research interests include secure computation, applied cryptography and big data security.

Background

In the era of Big Data, data has emerged as a critical resource in various industries. However, as data is often owned by multiple parties and distributed across different sources, privacy concerns arise when it comes to collaborative processing. Though sharing data between different entities can lead to greater value, the fear of privacy breaches often hinders such collaborative initiatives. Secure multiparty computation offers a solution to these issues by ensuring both the confidentiality of the input data and the accuracy of the final computation. By using protocols that don't involve a third party, this technique guarantees that the input data of all participants in the computation remains undisclosed, while at the same time enabling secure collaboration.

The problem of secure two-party comparison, which is a fundamental issue in secure multiparty computation, was originally presented by Yao. The two participants, Alice and Bob, with x and y as inputs, jointly execute the comparison function $f(x, y)$ in a way that does not reveal their respective inputs, and obtain the comparison results u_a and u_b, respectively, i.e. $(u_a, u_b) \leftarrow f(x, y)$. After its proposal, efficient solutions to secure two-party comparison have been discovered by researchers and applied in various fields, including secure sorting problems, interval proofs, and more. However, previous research has primarily focused on enhancing the efficiency of the protocol, neglecting the crucial concern of ensuring that Alice and Bob consistently obtain the same comparison result, such that $u_a = u_b$ always holds.

In this paper, we first propose a new paradigm for secure two-party comparison to solve the problem. Using the threshold Paillier cryptosystem, we develop a secure two-party comparison protocol that satisfies the new paradigm to ensure $u_a = u_b$. We demonstrate the security of the protocol under semi-honest conditions using a simulation paradigm, and prove that the protocol is resistant to chosen-plaintext attack. Experimentally, we compare existing secure two-party comparison schemes based on garbled circuits, homomorphic encryption and secret sharing. Theoretical analysis and experimental results show that our approach is computationally more efficient than existing protocols and guarantees $u_a = u_b$.

This study was supported by the National Key Research and Development Program of China (No. 2022YFB3102700) and the National Natural Science Foundation of China (No. 62202358, 62102295, 62072109, U1804263, 61632013).